IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

UNITED STATES OF AMERICA v. DALE BRITT BENDLER, Defendant.	Case No. 1:25-cr-00109-RDA

GOVERNMENT'S SENTENCING MEMORANDUM

Defendant Dale Bendler broke his oath to the United States and put cash before country when he decided to secretly lobby for foreign clients and mishandled classified materials during that work. Defendant's career began honorably—he served for years as a Central Intelligence Agency ("CIA") officer and retired in 2014 as a member of the Senior Intelligence Service.[1] He was then given the opportunity to rejoin the Agency as a full-time contractor while collecting his full pension. But Defendant still wanted more. So unlike other retired intelligence professionals who join the private sector *after* leaving public service, Defendant decided to do both jobs—and collect both salaries—at the same time. But even this was not enough. So Defendant decided to use his access to classified information and relationships with his colleagues to advance his lucrative lobbying career. There was only one problem with this profitable arrangement: it was blatantly illegal.

[1] The Senior Intelligence Service is a version of the federal civil service's Senior Executive Service that is intended to recruit and manage senior intelligence professionals in the U.S. intelligence community. Members of the Senior Intelligence Service are roughly equivalent to flag officers in the U.S. Armed Forces (*i.e.*, generals and admirals).

For three years, Defendant lied to and manipulated his CIA colleagues, the U.S. government, and the American public by hiding the fact that he was earning hundreds of thousands of dollars in fees from foreign lobbying clients while also working at the CIA. Defendant's crimes not only constituted a conflict of interest, but also compromised classified information, because in his quest to serve his private lobbying clients, Defendant abused his access to CIA information and resources. He shared classified information with foreign nationals and individuals who did not have U.S. security clearances or any other authorization to know such information. In Defendant's own words, his continued access to the CIA and his ability to abuse that access were what set him apart from other former intelligence community officials on the consultant circuit:

The client can benefit from my active status . . . because it means I am current, very current. I don't tell war stories about Timothy McVeigh, but instead what is happening today . . .

Defendant spent most of his life honorably serving America, but his breach of trust in his later years was significant, and he should be held accountable for his crimes. Accordingly, the Court should impose a below-Guidelines custodial sentence of 24 months, which is the maximum sentence the Government can recommend under the Plea Agreement. *See* ECF No. 8 ¶ 4.

APPLICABLE SENTENCING GUIDELINES

The Government agrees with the Sentencing Guidelines calculation in the Presentence Investigation Report ("PSR"). The counts in the Criminal Information group under § 3D1.2(b) because the United States Government is the victim of both crimes and Defendant's acts as a foreign agent while being a public official and mishandling of classified information were part of Defendant's scheme to use his position at the CIA to benefit himself and his foreign lobbying clients. *See* PSR ¶ 47. Therefore, the count with the highest offense level in the Information

should be used to calculate the Guidelines. Guidelines § 3D1.3(a). Here, that is Count Two in the Information which charged Defendant with the unauthorized removal and retention of classified documents or material, in violation of 18 U.S.C. § 1924. PSR ¶ 48.

Count One charged Defendant with acting as an agent of a foreign principal while being a public official, in violation of 18 U.S.C. § 219. The Appendix to the Guidelines identifies Guideline § 2C1.3 as the applicable Guideline for a Section 219 conviction. Guideline § 2C1.3 is titled, "Conflict of Interest; Payment or Receipt of Unauthorized Compensation," and starts with a base offense level of 6, which can be increased by four levels if the "offense involved actual or planned harm to the government." Here, Defendant's conduct harmed the U.S. government by wasting U.S. government resources, obstructing U.S. government functions, and compromising U.S. government classified information. Thus, if Defendant was only convicted of violating Section 219, the applicable offense level would be 10.

But Defendant also was convicted of violating 18 U.S.C. § 1924 (Count Two). No Guideline has been expressly promulgated for Section 1924, but under Guideline § 2X5.1, "the most analogous offense Guideline" is § 2M3.3. *See* PSR ¶ 48. As described further in the Government's response to Defendant's objections to Pretrial Services' Guidelines calculation, "[i]n determining which guideline is most analogous, the sentencing court must . . . look to the 'offense conduct charged in the count of the indictment or information of which the defendant was convicted.'" *United States v. Terry*, 86 F.3d 353, 357 (4th Cir. 1996). Here, the offense conduct charged in Count Two of the Information involved Defendant's mishandling and unauthorized disclosure of U.S. government information classified up to the SECRET level. *See* PSR, Addendum at 24-26. Therefore, as Pretrial Services concluded, Guideline § 2M3.3(a)(2) is the most analogous Guideline for Count Two and the base offense level is 24.

The Government also agrees with the two-level upward adjustment that the PSR recommends. As a CIA contractor with a Top Secret/Sensitive Compartmented Information ("TS/SCI") security clearance, Defendant abused his position of public trust in a manner that significantly facilitated the commission of his crimes. He had access to the resources, personnel, and information that he misappropriated to benefit his private lobbying clients because of his role in the U.S. intelligence community and his security clearance. Therefore, Guideline § 3B1.3 applies and the offense level should be increased by two more levels to 26. *See* PSR ¶ 51; *see also United States v. Kingsbury*, 107 F.4th 879, 881-82 (8th Cir. 2024) (upholding application of § 3B1.3 to TS/SCI clearance holder convicted of unlawfully retaining classified information relating to the national defense); *United States v. Ford*, 288 F. App'x 54, 60-61 (4th Cir. 2008) (per curiam) (same).

Lastly, the Government agrees with the PSR recommendation that Defendant should receive a three-level downward adjustment for acceptance of responsibility under Guidelines §§ 3E1.1(a) and (b), PSR ¶¶ 55-56, and an additional two-level downward adjustment as a zero-point offender under Guideline § 4C1.1, *id.* ¶ 54. With all of these adjustments, Defendant's total adjusted Guidelines offense level is 21 (37 to 46 months).

ARGUMENT

When considering the factors enumerated in 18 U.S.C. § 3553(a), Defendant deserves a sentence of 24 months, which the longest sentence the Government can recommend under the Plea Agreement.

I. Nature and Circumstances of the Offense

Defendant's breach of trust occurred at one of the most sensitive and secure buildings on the planet. While working as a full-time contractor at the CIA in the Eastern District of Virginia,

Defendant had employee-like access to CIA resources, information, and personnel. Plea Agreement, Statement of Facts ¶ 3. He also had a reputation that granted him influence within the CIA. Having served around the world as a CIA officer for over 30 years, Defendant had retired as a member of the Senior Intelligence Service. When he returned to the CIA as a contractor, he brought this reputational cachet with him. *Id.* ¶ 4. So when Defendant asked more junior officers questions or gave them advice, those officers deferred to Defendant and assumed that Defendant was an "old hand" of the Agency who knew how things worked and was acting in the best interests of the Agency. Defendant knew that he could influence less experienced members of the intelligence community, but instead of guiding them and providing sage advice, he manipulated and took advantage of them to enrich himself.

For example, in approximately 2017, Defendant began working for a foreign national who was being investigated by his home country for allegedly embezzling money from that country's sovereign wealth fund ("Foreign Principal 1" in the Information and Statement of Facts). *Id.* ¶ 7. Defendant was paid $20,000 per month to help Foreign Principal 1 mount a public relations campaign to rebut the embezzlement allegations and lobby U.S. government and foreign officials. *Id.* Upon learning of the possible consulting work, but before being hired, Defendant searched classified U.S. government computer systems to see what information, if any, was available related to Foreign Principal 1. *Id.* ¶ 8. These searches were unauthorized and Defendant had no legitimate work reason to conduct them.

Later that same day, Defendant sent the U.S. lobbying firm that was acting as an intermediary between Defendant and Foreign Principal 1 (the "U.S. Lobbying Firm" in the Information and Statement of Facts) a proposal that listed actions Defendant was willing to take to accomplish Foreign Principal 1's goals, including publishing online articles and messages to

influence the American public and using his prior relationships with government officials on the National Security Council and in the Office of the Director of National Intelligence to influence U.S. policy. Defendant also included classified U.S. government information, classified up to the SECRET//NOFORN level, in his proposal to Foreign Principal 1. *Id.* Despite his decades of training on how to properly handle and disseminate classified information, Defendant sent this proposal to U.S. Lobbying Firm over a commercial email provider and stored copies of the proposal on his personal electronic device and in his personal email account, neither of which was authorized to store or transmit classified information. *Id.*

After being hired, Defendant used his position at the CIA to try to influence U.S. government and foreign officials to benefit Foreign Principal 1 by influencing the foreign government's embezzlement investigation. *Id.* ¶¶ 9-11. Despite having multiple disclosure obligations as a CIA contractor and clearance holder, Defendant never told the CIA that he had been hired to influence the embezzlement investigation of Foreign Principal 1 or that he was being paid $20,000 per month for that work. Defendant also never made this information public by filing a registration statement with the Foreign Agents Registration Act ("FARA") Unit of the U.S. Department of Justice. The reason for Defendant's concealment was obvious: "he believed that if the true nature of his work were known, the effectiveness of his lobbying and public relations activities would be reduced and his contract with U.S. Lobbying Firm and Foreign Principal 1 might end." *Id.* ¶ 12. In total, Defendant was paid approximately $195,000 for his unauthorized and undisclosed work for Foreign Principal 1. *Id.* ¶ 11.

On another occasion, Defendant tried to influence U.S. government officials to establish a relationship with a different lobbying client ("Foreign Principal 2" in the Information and Statement of Facts) to help that client obtain a U.S. visa. *Id.* ¶¶ 13-14. Before Foreign Principal

2 hired Defendant, he had been denied a U.S. visa because of allegations that he was involved in laundering money for a foreign terrorist organization. *Id.* ¶ 13. "Using his past senior positions in the U.S. government and role as a CIA contractor, [D]efendant attempted to influence U.S. government officials' perceptions of Foreign Principal 2 and, at the same time and unbeknown to the U.S. government officials, coached Foreign Principal 2 on how he should interact with U.S. government officials." *Id.* ¶ 14. Defendant also abused his access to CIA systems and searched classified U.S. government databases to see what, if any, information was available related to Foreign Principal 2. *Id.* Defendant also shared non-public and sensitive U.S. government information with Foreign Principal 2 and U.S. Lobbying Firm (which, again, worked as an intermediary between Defendant and Foreign Principal 2). *Id.* ¶ 17. Defendant never told the CIA that Foreign Principal 2 had hired him to resolve the terrorism financing allegations and to obtain him a U.S. visa. *Id.* Nor did he tell the CIA that Foreign Principal 2 had paid him approximately $10,000 for his work. *Id.* Unsurprisingly, he never filed a registration statement with the FARA Unit for his work for Foreign Principal 2.

From July 2017 until September 2020 (when the CIA terminated his contract and revoked his security clearance), Defendant worked for numerous private clients, including many foreign nationals, and abused his access to classified U.S. government computer systems to search for information about those clients. *Id.* ¶ 20. "In a handful of incidents, [D]efendant also removed classified information from the CIA, placed that information on his own personal electronic devices, and disclosed that information, classified up to the SECRET//NOFORN level, to individuals who were not authorized to know such information, including individuals whom he was trying to convince to hire him as a consultant." *Id.* ¶ 21. In total, between July 2017 and September 2020, Defendant earned approximately $360,000 in private client fees while also

working as a full-time CIA contractor with daily access to highly classified material that he searched like it was his own personal Google. *Id.* ¶ 23. He violated his oaths, broke the law, and should be held accountable.

II. The Need for Adequate Deterrence and Protecting the Public

While working at the CIA, Defendant was granted access to some of the U.S. government's most sensitive secrets and programs. He promised to keep this information secret for life. While Defendant unfortunately broke that promise, the vast majority of former members of the intelligence community honor their commitments after leaving the government and are able to live productive post-public service lives while keeping the information they learned during their public service secret. To ensure that former clearance holders are not tempted to break their oaths and jeopardize national security after they leave government service, it is important for Defendant to serve a significant custodial sentence that will deter others from making similar choices.

The need for general deterrence is especially important in the intelligence world because many of the activities of the intelligence community are cloaked in secrecy and even those who have the appropriate security clearances are not given access to the type of information that normally would allow potential wrongdoing to be identified and investigated. For example, Defendant committed his crimes while working in a secure U.S. government building in the Eastern District of Virginia. *Id.* ¶ 3. Access to that building was restricted. He also used classified U.S. government computer systems and information to further his criminal activity. *Id.* ¶¶ 8, 14, 20, 22. Because many of the locations, systems, and information that Defendant used to commit his crimes were classified, investigating his criminal activity presented challenges stemming from restrictions regarding the proper handling and access to classified

systems and information. This is one of the practical consequences of secrecy. In many ways, Defendant was able to use the fact that his job was so sensitive and classified as both a sword and a shield. He wielded it as a sword when he abused his access to classified information and he relied on it as a shield to hide his criminal activity. The dualism of secrecy inherent in Defendant's job is another reason why it is important to send a strong message at sentencing and deter other former members of the intelligence community from breaking the law to make some extra money.

A significant sentence also is warranted because Defendant, who still has decades of highly classified information in his head, needs to be deterred from sharing that information in the future with unauthorized recipients, including any other wealthy clients who may be interested in liberating some of that information in exchange for money or a cushy "consulting" arrangement.

Lastly, a meaningful sentence is important to protect the public. The CIA is responsible for collecting foreign intelligence information that reveals the plans, intentions, and capabilities of the United States' adversaries and for conducting clandestine actions, at the direction of the President of the United States, designed to preempt threats or achieve U.S. policy objectives. Crim. Info. ¶ 1. In the CIA's own words, its "mission is straightforward but critical: leverage the power of information to keep our Nation safe."[2] Whether covertly exfiltrating U.S. State Department employees from Iran in 1980, recovering a Soviet submarine from the ocean floor, or smuggling pocket-sized versions of *Dr. Zhivago* into the Soviet Union,[3] the CIA and its workforce strive every day to keep the American public safe. Part of how they do that is by

[2] https://www.cia.gov/about/.

[3] https://www.cia.gov/legacy/museum/the-debrief/behind-the-artifact-operations/.

protecting the secrets that they gather, as well as the sources and methods through which they collect those secrets. The classification system and the laws that criminalize the unauthorized disclosure of classified information are intended to protect that information. When individuals, like Defendant, break those laws and share classified information outside of the approved channels, they jeopardize national security and make it harder for the CIA, and the larger intelligence community, to protect the American public.

III. Defendant's History and Characteristics

Defendant is a career public servant. Except for four years of college, from 1975 until he was terminated by the CIA in 2020, Defendant served honorably in the U.S. military and intelligence community. PSR ¶¶ 81, 85. He is highly educated with a Master's Degree from the U.S. Naval War College and highly trained by the U.S. government. *Id.* ¶¶ 75, 85. According to the PSR, he had a loving and supportive upbringing and his family life is stable. *Id.* ¶¶ 64-71. His career of public service and age are mitigating factors which warrant a below-Guidelines sentence.

IV. Seriousness of the Offense, Just Punishment, and Respect for Law

Defendant's crimes not only represent a breach of trust, but they also put classified information at risk by sharing it with unauthorized recipients and storing it on unauthorized media. The classified and sensitive impact statements which were filed concurrently with this brief through the Classified Information Security Officer further describe the seriousness of Defendant's unauthorized disclosures. *See* ECF No. 24.

While the Guidelines recommend a sentence of 37 to 46 months for Defendant, a lower sentence of 24 months is warranted here. Once he was caught and confronted, Defendant began to gradually accept responsibility for his actions. He sat down with the government for multiple

proffers between June and November 2024 and ultimately agreed to a pre-indictment resolution. In April 2025, he pleaded guilty via a plea agreement to a two-count Criminal Information. ECF No. 7. Pursuant to the Plea Agreement, Defendant has already made a forfeiture payment to the U.S. government of $85,000. ECF No. 8, Plea Agreement ¶ 9. He also has submitted filings to the FARA Unit for his registrable activities on behalf of foreign principals. *Id.* ¶ 11(C). Accordingly, a below-Guidelines 24-month sentence would be a just punishment.

V. Avoid Unwarranted Sentencing Disparities

A sentence of 24 months would be well within the range of sentences in analogous cases. According to the U.S. Sentencing Commission's Interactive Data Analyzer, between 2015 and 2024, 13 cases were sentenced using Guideline § 2M3.3.[4] The average sentence from those cases was 53 months. The median sentence was 46 months. Of those 13 cases, only 23.1% of the defendants received sentences of less than two years. The other 77% received sentences ranging from two years to ten years.

Before 2018, 18 U.S.C. § 1924 was a misdemeanor, but in 2018 Congress changed it to a felony with a five-year statutory maximum punishment. *See* Pub. Law 115-118, Sec. 202. Since then, there have been only a handful of cases where defendants have pleaded guilty to violating 18 U.S.C. § 1924. In those cases, defendants' sentences have been lower than the sentencing averages reported in the U.S. Sentencing Commission's data for Guideline § 2M3.3. For example, in *United States v. Ashby*, Case No. 1:24-cr-00055 (S.D. Ga.), the defendant was a U.S. Department of Defense employee who pleaded guilty pre-indictment to a single count of Section 1924 for removing classified documents from their authorized location. She was sentenced to 36 months in prison. In *United States v. Gun*, Case No. 1:24-cr-00199 (E.D. Va.),

[4] *See* ida.ussc.gov.

the defendant was a U.S. Department of Defense employee who pleaded guilty to a single count of Section 1924 for removing two classified documents from their authorized location. He was sentenced to 18 months in prison. *See also United States v. Kemp*, Case No. 3:21-cr-00009 (S.D. Ohio) (received 12 months and a day prison sentence for pre-indictment guilty plea to a single count of 18 U.S.C. § 1924).

In contrast, sentences for convictions under 18 U.S.C. § 793 tend to be much higher than sentences for convictions under 18 U.S.C. § 1924, even though the applicable Guideline for both types of convictions may be § 2M3.3.[5] *See, e.g.*, *United States v. Schena*, Case No. 1:24-cr-00158 (E.D. Va.) (sentenced to 48 months for 793 conviction); *United States v. Rahman*, Case No. 1:24-cr-00249 (E.D. Va.) (37 months); *United States v. Schultz*, Case No. 3:24-cr-0056 (M.D. Tenn.) (84 months); *United States v. Teixeira*, Case No. 1:23-cr-10159 (D. Mass.) (180 months); *United States v. Birchum*, Case No. 8:23-cr-00032 (M.D. Fla.) (36 months); *United States v. McLean*, Case No. 3:22-cr-00115 (M.D. Fla.) (120 months)[6]; *United States v. Kingsbury*, Case No. 4:21-cr-00101 (W.D. Mo.) (46 months); *United States v. Hale*, Case No. 1:19-cr-00059 (E.D. Va.) (45 months); *United States v. Franklin*, Case No. 1:05-cr-00225 (E.D. Va.) (120 months).

Although the Section 1924 conviction should drive the sentence in this case, Defendant also pleaded guilty to violating 18 U.S.C. § 219 by acting as an agent of foreign principals while also being a public official. The statutory maximum penalty for a violation of Section 219 is two years' imprisonment. Section 219 prosecutions are rare; to date, the only defendant to have been

[5] For 793 convictions, the applicable Guideline may alternatively be § 2M3.2 which is titled, "Gathering National Defense Information" and begins at a base offense level of 35 for top secret information and 30 for other types of national defense information.

[6] McLean was also sentenced to 160 months for distributing child sexual abuse material. His sentences are running concurrently.

convicted was former U.S. Senator Robert Menendez. *See United States v. Menendez et al.*, Case No. 1:23-cr-00490 (S.D.N.Y.). In July 2024, Menendez was convicted at trial for engaging in bribery and obstruction of justice and for violating Section 219 through a scheme to use his public office to benefit the Government of Egypt in exchange for cash, gold bars, and other things of value. In January 2025, Menendez was sentenced to 132 months' imprisonment, including the statutory maximum 24 months of imprisonment on the Section 219 charge.

CONCLUSION

Corruption can happen anywhere, but when it happens in the secretive world of intelligence, it must be rooted out because the stakes are so high. For intelligence agencies to be effective, their work must mostly be done in the shadows, far from the public's gaze. Intelligence agencies like the CIA are given a great deal of trust by the American people to follow the law and to act in the public's best interest. That trust is given, however, with the expectation that if it is broken, the consequences will be substantial. This is because many of the normal mechanisms that keep public officials honest, like public records laws, public hearings, elections, etc., do not apply to the intelligence world. Severity is also warranted because the public trust is fragile and can be lost easily. When a member of the intelligence community breaks the law, the public may question whether the secrecy that surrounds intelligence work allowed the criminal conduct to occur in the first place or, at a minimum, to go on longer than it otherwise would have. Therefore, to preserve the trust that the American people place in the intelligence community, when members of that community break the law, the consequences must be significant. Accordingly, for the reasons stated above, the United States recommends that the Court impose a sentence of 24 months in prison, which is the highest recommendation the Government can make under the Plea Agreement.

Respectfully submitted,

Erik S. Siebert
United States Attorney

By: s/ *Gordon D. Kromberg*

Gordon D. Kromberg
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
Tel: (703) 299-3721
Gordon.Kromberg@usdoj.gov

s/ *Adam P. Barry*
Adam P. Barry, Cal. Bar No. 294449
Acting Deputy Chief
Heather M. Schmidt
Senior Trial Attorney
National Security Division
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, D.C. 20530
Tel: (202) 233-0788
Adam.Barry@usdoj.gov

Attorneys for the United States

CERTIFICATE OF SERVICE

I hereby certify that on September 17, 2025, I filed the foregoing Memorandum using the Court's CM/ECF system, which will send notice to all registered parties.

s/ *Adam P. Barry*

Acting Deputy Chief